Authentication Service and Secure Communications for Wireless Networks

著者	陸 ?
その他のタイトル	無線ネットワークにおける認証サービスと安全な通信方式に関する研究
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2013
報告番号	12102甲第6859号
URL	http://hdl.handle.net/2241/00122390

（博甲）

氏　名（本籍）	陸　璜（リク　コウ）　（中国）
学 位 の 種 類	博　士（工学）
学 位 記 番 号	博　甲　第　6859　号
学位授与年月日	平成２６年　３月２５日
学位授与の要件	学位規則第４条第１項該当
審 査 研 究 科	システム情報工学研究科
学位論文題目	Authentication Service and Secure Communications for Wireless Networks（無線ネットワークにおける認証サービスと安全な通信方式に関する研究）

主　　査	筑波大学　教授	博士(工学)	李　頡
副　　査	筑波大学　教授	工学博士	岡本 栄司
副　　査	筑波大学　教授	博士(理学)	加藤 和彦
副　　査	筑波大学　准教授	工学博士	片岸 一起
副　　査	筑波大学　准教授	博士(情報科学)	木村 成伴
副　　査	公立はこだて未来大学　教授	博士(工学)	姜 暁鴻

論　文　の　要　旨

本論文では、重要な無線通信ネットワークであるクラスタベース無線センサネットワーク（Cluster-based Wireless Sensor Networks）と車両間アドホックネットワーク（Vehicular Ad Hoc Networks）における認証サービスと安全な通信方式について研究を行った。論文の第１章と第２章では、研究の背景と関連研究と研究の位置付け及び研究の目的について述べた。第３章では、ID ベースデジタル署名方式を用いたクラスタベース無線センサネットワークにおける安全の経路選択プロトコルを提案した。第４章では、ID ベースデジタル署名と ID ベースオンライン・オフラインデジタル署名の二つの方式をそれぞれ用いて、二つの安全かつ効率的なデータ通信プロトコルを提案した。提案したプロトコルでは、そのセキュリティは ID ベース暗号系に基づくため、補助的なデータ通信をせずに該当する秘密鍵を取得することが可能であり、安全かつ効率的にデータ通信を行うことを可能にした。シミュレーションにより、提案したプロトコルの有効性を示した。第５章では、車両間アドホックネットワークのプライバシーを保護する認証機構について調べた。第 6 章では、車両間アドホックネットワークにおける動的なプライバシー保護のための ID ベース認証フレームワークを新たに提案した。提案したフレームワークの認証とプライバシーの機能について調べ、性能評価を行い、その有効性を示した。第 7 章では、車両間アドホックネットワークにおける条件付きプライバシー保護と否認防止機能を持つ認証フレームワークを提案した。提案した認証フレームワークでは、ID ベースデジタル署名と ID ベースオンライン・オフラインデジタル署名の二つの方式を路側機と車両間の認証および車々間の認証にそれぞれ利用され、否認防止のための追跡機能を持ちながら、条件付きプライバシー保護機能も実現した。第 8 章では、論文の研究をまとめ、今後の課題について述べた。

審　査　の　要　旨

【批評】

無線情報通信ネットワークにおける安全性と性能を向上させることは重要な課題である。本論文では、特に、無線情報通信ネットワークであるクラスタベース無線センサネットワークと車両間アドホックネットワークにおける効率的な認証サービスと安全な通信方式について研究を行った。

本論文では、既存の ID ベースデジタル署名方式と ID ベースオンライン・オフラインデジタル署名方式を用いて、クラスタベース無線センサネットワークにおける安全かつ効率的なデータ通信プロトコルを新たに提案した。提案したプロトコルのセキュリティの要件と様々なセキュリティ攻撃に対する対処法について調べた。シミュレーションにより、提案したプロトコルの有効性を明らかにした。また、車両間アドホックネットワークにおけるプライバシーを保護するための ID ベース認証フレームワークと条件付きプライバシー保護と否認防止機能を持つ認証フレームワークを新たに提案し、セキュリティ評価とシミュレーションにより、提案したフレームワークの有効性を示した。

これらの研究は、情報通信ネットワークシステムのセキュリティと性能の向上に対して情報工学上、貢献するところが大きいと判断される。今後は、無線ネットワークシステム上に実装し、より現実的な情報通信ネットワークシステムの環境で、提案したデータ通信プロトコルと認証フレームワークの有効性と実用性を示すことが望まれる。

【最終試験の結果】

平成 26 年 1 月 30 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。